CLAIMS

1. A method in a computer system for securing data stored on a storage device, the computer system having a redirection driver, available storage, and redirected storage, comprising:

receiving a request to access a portion of data on the storage device, the request referring to an original location on the storage device;

under control of the redirection driver,

intercepting the request to access the data;

determining whether the request refers to an original location that has previously been redirected to redirected storage;

when the request refers to an original location that has previously been redirected to redirected storage, using a location in redirected storage as a current redirected location, otherwise allocating available storage to a new location in redirected storage and using the new location as the current redirected location; and

redirecting the access request to refer to the current redirected location, such that the request transparently accesses the current redirected location instead of the original location; and

restarting the computer system from a powered-down state, wherein the data stored in the original location on the storage device remains unaltered, without any restorative copying of data.

2. A computer system for securing data stored on a storage device, comprising:

data access request that refers to an original location on the storage device;

available storage; and

redirection driver, installed in the computer system during power-up initialization, that,

automatically intercepts the data access request; and

redirects the access request to access a redirected location in the available storage, such that a requested modification at the original location is not performed and is instead performed to the redirected location, and such that, when the computer system is restored from a powered-down state, the data in the original location on the storage device remains unaltered without any restorative copying.

3. A method in a computer system for protecting data stored in a portion of a storage device having a designated protected space, the computer system having a redirected space, comprising:

intercepting a request from requesting code to access a location in the protected space of the storage device; and

determining a location in the redirected space that is associated with the location in the protected space; and

redirecting the intercepted request to access the determined location in the redirected space instead of the location in the protected space, in a manner that is transparent to the requesting code, so that the data stored in the location in the protected space remains unaltered.

4. The method of claim 3 wherein a redirection driver performs the intercepting the request, determining the location in the redirected space, and redirecting the intercepted request.

5. The method of claim 4 wherein the driver is inserted into a driver hierarchy that is controlled by an operating system of the computer system.

6. The method of claim 3 wherein the designated protected space of the storage device comprises the entire storage device.

7. The method of claim 3 wherein the determined location in the redirected space resides in the storage device.

8. The method of claim 3 wherein the determined location in the redirected space resides in an other storage device.

9. The method of claim 3 wherein the request to access a location in the protected space is a request to read from the protected space.

10. The method of claim 9 wherein the redirecting the intercepted read request results in automatically reading data from the determined location in the redirected space instead of from the location in the protected space.

11. The method of claim 3 wherein the request to access a location in the protected space is a request to write to the protected space.

12. The method of claim 11 wherein the redirecting the intercepted write request results in automatically writing data to the determined location in the redirected space instead of to the location in the protected space.

13. The method of claim 11 wherein the redirecting the intercepted write request results in automatically allocating available space to use as new redirected space and writing data to a location in the new redirected space.

14. The method of claim 3 wherein the determining the location in the redirected space that is associated with the location in the protected space further comprises first allocating available space to be used as the redirected space.

15. The method of claim 3 wherein the storage device is one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, and a semi-persistent storage device.

16. The method of claim 3 wherein the location in the protected space refers to at least one of a sector, a group of sectors, a cluster, and a group of clusters.

17. The method of claim 3 wherein the location in the redirected space refers to at least one of a sector, a group of sectors, a cluster, a group of clusters, a virtual cluster, and a group of virtual clusters.

18. The method of claim 17 wherein the sector is a logical sector.

19. The method of claim 17 wherein the sector is a physical sector.

20. The method of claim 17 wherein the location in the protected space refers to a sector.

21. The method of claim 17 wherein the location in the protected space refers to an abstraction of storage that is larger than a sector.

22. The method of claim 3 wherein the redirected space is organized according to a combination of different storage units.

23. The method of claim 22 wherein a portion of the redirected space is organized as one of virtual clusters, clusters, files, and sectors, and an other portion is organized according to a different storage unit.

24. The method of claim 3, further comprising:

designating a portion of the storage device as unprotected space;

intercepting a request to access a location in the unprotected space of the storage device;

performing the request without redirection to access the unprotected space.

25. The method of claim 3, further comprising:

receiving a request to shutdown the computer system; and

upon receiving the request to shutdown the computer system,

disregarding the data in the redirected space, so that when the computer system is rebooted, the data in the protected space of the storage device appears unaltered.

26. The method of claim 25 wherein disregarding the data in the redirected space comprises at least one of deleting the data from the storage in the redirected space, disassociating the redirected space from the protected space, and ignoring the data in the redirected space.

27. The method of claim 3, further comprising:

receiving a request to shutdown the computer system; and

upon receiving the request to shutdown the computer system,

saving the data stored in the redirected space.

28. The method of claim 27 wherein saving the data stored in the redirected space comprises copying the data from the redirected space to associated locations in the protected space, thereby making permanent the data that was redirected to the redirected space.

29. The method of claim 27 wherein saving the data stored in the redirected space comprises saving the association between the protected space and the redirected space without copying the data from the redirected space.

30. The method of claim 3, further comprising using redirection tables to associate locations in the protected space to locations in the redirected space.

31. The method of claim 30 wherein the redirection tables comprise at least one of a protected space redirection table, an available space table, and an unprotected space table.

32. A computer-readable memory medium containing instructions that control a computer processor to protect data stored in a portion of a storage device having a designated protected space, the computer system having a redirected space, by:

intercepting a request from requesting code to access a location in the protected space of the storage device; and

determining a location in the redirected space that is associated with the location in the protected space; and

redirecting the intercepted request to access the determined location in the redirected space instead of the location in the protected space, in a manner that is transparent to the requesting code, so that the data stored in the location in the protected space remains unaltered.

33. The computer-readable memory medium of claim 32 wherein the designated protected space of the storage device comprises the entire storage device.

34. The computer-readable memory medium of claim 32 wherein the determined location in the redirected space resides in the storage device.

35. The computer-readable memory medium of claim 32 wherein the determined location in the redirected space resides in an other storage device.

36. The computer-readable memory medium of claim 32 wherein the request to access a location in the protected space is a request to read from the protected space that results in automatically reading data from the determined location in the redirected space instead of from the location in the protected space.

37. The computer-readable memory medium of claim 32 wherein the request to access a location in the protected space is a request to write to the protected space that results in automatically writing data to the determined location in the redirected space instead of to the location in the protected space.

38. The computer-readable memory medium of claim 37 wherein the redirecting the intercepted write request results in automatically allocating available space to use as new redirected space and writing data to a location in the new redirected space.

39. The computer-readable memory medium of claim 32 wherein the determining the location in the redirected space that is associated with the location in the protected space further comprises first allocating available space to be used as the redirected space.

40. The computer-readable memory medium of claim 32 wherein the storage device comprises one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, and a semi-persistent storage device.

41. The computer-readable memory medium of claim 32 wherein the location in the protected space refers to at least one of a sector, a group of sectors, a cluster, and a group of clusters.

42. The computer-readable memory medium of claim 32 wherein the location in the redirected space refers to at least one of a sector, a group of sectors, a cluster, a group of clusters, a virtual cluster, and a group of virtual clusters.

43. The computer-readable memory medium of claim 42 wherein the location in the protected space refers to a sector.

44. The computer-readable memory medium of claim 42 wherein the location in the protected space refers to an abstraction of storage that is larger than a sector.

45. The computer-readable memory medium of claim 32 wherein the redirected space is organized according to a combination of different storage units.

46. The computer-readable memory medium of claim 45 wherein a portion of the redirected space is organized as at least one of virtual clusters, clusters, files, and sectors, and an other portion is organized according to a different storage unit.

47. The computer-readable memory medium of claim 32, further comprising:

designating a portion of the storage device as unprotected space;

intercepting a request to access a location in the unprotected space of the storage device;

performing the request without redirection to access the unprotected space.

48. The computer-readable memory medium of claim 32, further comprising:

receiving a request to shutdown the computer system; and

upon receiving the request to shutdown the computer system,

disregarding the data in the redirected space, so that when the computer system is rebooted, the data in the protected space of the storage device appears unaltered.

49. The computer-readable memory medium of claim 48 wherein disregarding the data in the redirected space comprises at least one of deleting the data from the storage in the redirected space, disassociating the redirected space from the protected space, and ignoring the data in the redirected space.

50. The computer-readable memory medium of claim 32, further comprising:

receiving a request to shutdown the computer system; and

upon receiving the request to shutdown the computer system,

saving the data stored in the redirected space.

51. The computer-readable memory medium of claim 50 wherein saving the data stored in the redirected space comprises copying the data from the redirected space to associated locations in the protected space, thereby making permanent the data that was redirected to the redirected space.

52. The computer-readable memory medium of claim 50 wherein saving the data stored in the redirected space comprises saving the association between the protected space and the redirected space without copying the data from the redirected space.

53. The computer-readable memory medium of claim 32, further comprising using redirection tables to associate locations in the protected space to locations in the redirected space.

54. A computer system for protecting data stored in a portion of a storage device, comprising:

protected space designated on the storage device for storing the protected data;

redirected storage space in the computer system designated for storing attempted modifications of the protected data;

redirection driver, installed in the computer system, that

intercepts requests to access locations in the protected space;

redirects intercepted requests so that the requests result in accessing locations in the redirected storage space instead of locations in the protected space, thereby leaving the protected space unaltered.

55. The computer system of claim 54 wherein the protected space remains unaltered through a reboot of the computer system, without any restorative copying of the protected data.

56. The computer system of claim 54, further comprising a redirection table that maps locations in the protected space to locations in the redirected storage space, and is used by the redirection driver to determine a location in the redirected storage space to use for redirecting an intercepted request.

57. The computer system of claim 56 wherein the contents of the redirection table are saved by the computer system when the computer system is powered down.

58. The computer system of claim 54 wherein the protected space comprises the entire storage device and the redirected storage space is not located on the storage device.

59. The computer system of claim 54 wherein the redirected storage space is located on the storage device.

60. The computer system of claim 54 wherein an intercepted and redirected access request is a request to read from a location in the protected space.

61. The computer system of claim 54 wherein an intercepted and redirected access request is a request to write to a location in the protected space that is redirected to modify a location in the redirected space.

62. The computer system of claim 54 wherein the storage device is one of a hard disk drive, a read/write CD ROM drive, a floppy disk drive, and a semi-persistent storage device.

63. The computer system of claim 54 wherein the redirection driver refers to the redirected storage space in at least one of files, clusters, virtual clusters, and sectors of data.

64. The computer system of claim 54 wherein the redirection driver refers to the redirected storage space using multiple data addressing abstractions.

65. The computer system of claim 54 wherein the redirection driver implements a virtual cluster data abstraction.

66. The computer system of claim 54 wherein the redirection driver is installed by inserting the redirection driver into a chain of drivers so that it is automatically invoked by the computer system.

67. The computer system of claim 54, further comprising:

unprotected space designated on the storage device for allowing modifications to a portion of the storage device.

68. The computer system of claim 67 wherein the redirection driver disregards access requests to the unprotected space.

69. The computer system of claim 67 wherein the redirection driver intercepts and redirects access requests to access locations in the unprotected space so that access to the unprotected data are also redirected.

70. The computer system of claim 67, further comprising an unprotected space table for tracking the locations of the storage device that are designated as unprotected space.

71. The computer system of claim 54 wherein the contents of the redirected storage space are saved by the computer system when the computer system is powered down.

72. A method for securing data in a storage device of a computer system having an operating system and a device driver, comprising:

installing a redirection driver before the device driver in a calling sequence of the operating system, so that the operating system invokes the redirection driver in response to receiving a request to access the storage device;

under control of the redirection driver,

intercepting a request to access a location on the storage device; and

redirecting the request to access a location in unused storage, such that the data in the location on the storage device remains unaltered;

restarting the computer system from a powered-down state, wherein the data stored in the location on the storage device remains unaltered, without requiring restorative copying of data.

73. The method of claim 72 wherein the redirection driver cannot be uninstalled by a user without special access privileges, thereby forcing the data to be securely maintained.

74. The method of claim 72, the device driver comprising one of a plurality of device drivers that are arranged in a layered fashion, and wherein the redirection driver is installed between two of these device drivers.

75. The method of claim 74 wherein each driver layer comprises a driver that communicates with an associated device according to different data abstraction; and wherein the redirection driver can be configured to be installed at different layers depending upon the data abstraction implemented by the redirection driver.

76. The method of claim 72 wherein the redirection driver handles blocks of data defined as at least one of virtual clusters, clusters, sectors, and files.

77. The method of claim 72 wherein the redirection driver handles multiple different data abstractions.

78. The method of claim 72 wherein the computer system comprises redirection tables that are maintained by the redirection driver to manage associations between data that has been redirected by redirecting the access request to the location in unused storage and unaltered data stored on the storage device.

79. A storage access redirection system for securing data in designated locations on a storage device in a computer system comprising:

available space table;

protected space redirection table; and

redirection driver, installed in the computer system, that

automatically intercepts a request to access one of the designated locations;

uses the protected space redirection table to determine whether the designated location has been previously redirected;

when it is determined that the designated location has been previously redirected, determines an associated redirected location; and

redirects the access request to the associated redirected location so that data in the designated location remains unaltered.

80. The storage access redirection system of claim 79, further comprising:

unprotected space table that is used to designate unprotected locations on the storage device that can be altered, wherein the redirection driver intercepts requests to access locations referred to by the unprotected space table and disregards them so that data in the unprotected locations on the storage device is modified according to the access requests.

81. The storage access redirection system of claim 79 wherein the request to access one of the designated locations is a read request.

82. The storage access redirection system of claim 79 wherein the request to access one of the designated locations is a write request.

83. The storage access redirection system of claim 82 wherein the redirection driver, when it is determined that the designated location has not been previously redirected, uses the available space table to allocate a new redirected location, uses the protected space redirection table to map the new redirected location to the designated location, and determines the new redirected location as the associated redirected location.